PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344207

(43)Date of publication of application : 14.12.2001

(51)Int.Cl. G06F 15/00
G06F 15/16
G06F 15/163
H04L 9/32
H04L 12/22

(21)Application number : 2000-162507

(22)Date of filing : 31.05.2000

(71)Applicant : NEC CORP

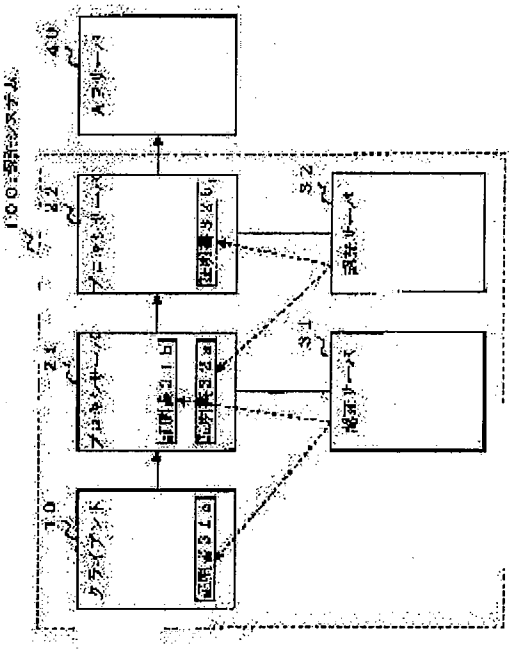
(72)Inventor : YOKOI HIDEHIKO

(54) CERTIFICATION SYSTEM AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To solve such a conventional problem that each certification server should be provided with a specific function for transferring a registered user s certificate between certification servers.

SOLUTION: In the certification system 100 constituted of a client 10 connected to a communication line, plural proxy servers 21, 22 interposed between the client 10 and a server 40 and plural certification servers 31, 32 formed correspondingly to respective proxy servers 21, 22, the servers 31, 32 respectively execute certification on the basis of certificates distributed to the corresponding proxy servers 21, 22 and the connection sources of the servers 21, 22. The proxy server 21 repeating the client 10 and the proxy server 22 transfers a certificate 31a owned by the client 10 to the proxy server 22. Thereby it is unnecessary to transfer the registered user's certificate between the certification servers 31, 32.



LEGAL STATUS

[Date of request for examination] 13.04.2001

[Date of sending the examiner's decision of rejection] 07.12.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－344207
（P2001－344207A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ	５Ｂ０４５
	15/16	６２０		15/16	６２０Ｂ	５Ｂ０８５
	15/163	６５０		15/163	６５０Ｘ	５Ｊ１０４
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｄ	５Ｋ０３０
	12/22			11/26		

審査請求　有　　請求項の数6　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－162507(P2000－162507)

(22)出願日　平成12年５月31日(2000.5.31)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

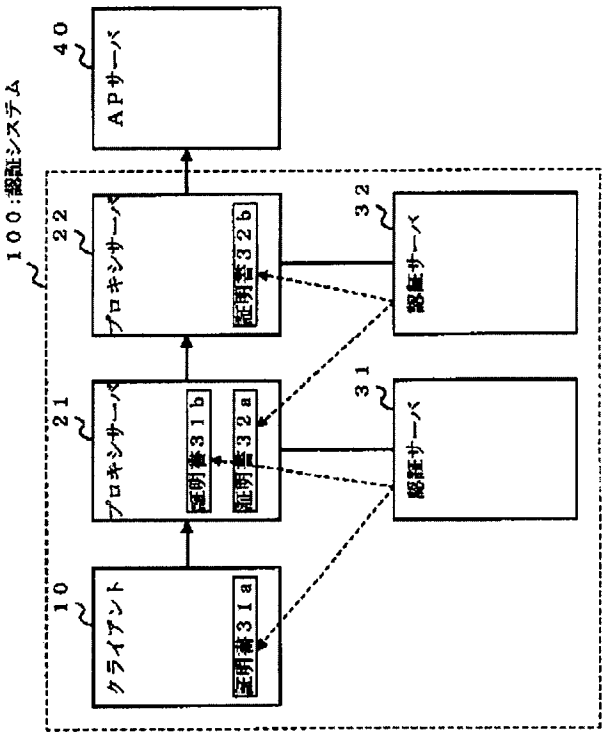
(72)発明者　横井　英彦
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　100086759
弁理士　渡辺　喜平

Ｆターム(参考)　5B045 BB19 BB28 BB47 BB48 GG09
5B085 AE23 BG07
5J104 AA07 BA02 KA01 MA03 PA07
5K030 GA15 HC01

(54)【発明の名称】　認証システムおよび認証方法

(57)【要約】
【課題】　登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能が各認証サーバに備わっていなければならなかった。
【解決手段】　通信回線に接続されたクライアント１０、クライアント１０とサーバ４０との間に介在する複数のプロキシサーバ２１，２２、それぞれのプロキシサーバに対応して設けられた複数の認証サーバ３１，３２とにより構成される認証システム１００において、認証サーバ３１，３２は、対応するプロキシサーバ２１，２２とこのプロキシサーバ２１，２２の接続元とに配布した証明書に基づいて認証を行う。そして、クライアント１０とプロキシサーバ２２とを中継するプロキシサーバ２１が、クライアント１０が保有する証明書３１ａをプロキシサーバ２２に受け渡す。その結果、登録されたユーザの証明書を認証サーバ間で受け渡す必要がなくなる。



【特許請求の範囲】
【請求項１】　通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに、対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとを具備する認証システムであって、
上記認証サーバは、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、
上記プロキシサーバは、接続先から上記クライアントに証明書を要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、
上記クライアントは、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信することを特徴とする認証システム。
【請求項２】　上記請求項１に記載の認証システムにおいて、
上記サーバに最も近いプロキシサーバは、接続元との間の認証が完了したとき、この接続元へ上記証明書要求を送信することを特徴とする認証システム。
【請求項３】　上記請求項１あるいは請求項２のいずれかに記載の認証システムにおいて、
上記プロキシサーバは、上記クライアントに配布された上記証明書とあわせて、自らに配布された上記証明書を接続先へ送信することを特徴とする認証システム。
【請求項４】　上記請求項１～請求項３のいずれかに記載の認証システムにおいて、
上記プロキシサーバは、自らに配布された上記証明書を上記証明書要求に添付して接続元へ送信し、
上記クライアントは、上記プロキシサーバに配布された上記証明書を確認して、配布された上記証明書を接続先へ送信することを特徴とする認証システム。
【請求項５】　上記請求項１～請求項４のいずれかに記載の認証システムにおいて、
上記クライアントは、上記サーバへの接続を要求してから所定時間内に上記証明書要求を入手することができないとき、自らに配布された証明書の引き渡しを中止することを特徴とする認証システム。
【請求項６】　通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに、対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとにより構成される認証方法であって、
上記認証サーバにて、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、
上記プロキシサーバにて、接続先から上記クライアントに証明書を要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、
上記クライアントにて、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信することで認証を行うことを特徴とする認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、認証システムおよび認証方法に関し、特に、通信回線に接続されたクライアント、クライアントとサーバとの間に介在する複数のプロキシサーバおよびこれらのプロキシサーバに対応して設けられた複数の認証サーバとにより構成される認証システムおよび認証方法に関する。
【０００２】
【従来の技術】従来より、この種の認証システムは、通信回線に接続されたクライアント、クライアントとサーバとの間に介在する複数のプロキシサーバおよび複数の認証サーバとにより構成されている。複数の認証サーバは、それぞれのプロキシサーバに対応して設けられている。そして、予め、すべてのプロキシサーバに属する認証サーバはクライアントを使用するユーザを登録するとともに、クライアントへ証明書を配布する。その上で、配布した証明書に基づいて、認証サーバが対応するプロキシサーバとこの接続元との間の認証をクライアント側から順番に行う。その結果、各プロキシサーバにてクライアントを使用するユーザを認証することが可能となる。しかし、すべての認証サーバからクライアントに証明書を配布しなければならないため、ユーザの管理だけで多大な作業が必要になる。
【０００３】この作業を軽減させるため、クライアントに最も近い認証サーバにだけユーザを登録させる構成とした認証システムも知られている（特開平１１－３２８１１７号公報）。この認証システムは、登録されたユーザの証明書を認証サーバ間で受け渡していくことで、プロキシサーバとこの接続元との間の認証をクライアント側から順番に行う。これは、クライアントと各プロキシサーバとの認証が行われる際に、各認証サーバでユーザの証明書が必要となるためである。すると、認証サーバすべてにクライアントのユーザ情報を登録しなくても、各プロキシサーバにてクライアントを使用するユーザを認証することが可能となる。
【０００４】
【発明が解決しようとする課題】しかしながら、上述した従来の認証システムにおいては、登録されたユーザの

証明書を認証サーバ間で受け渡していくという特別の機能が各認証サーバに備わっていなければならなかった。

【０００５】本発明は、上述の課題にかんがみてなされたもので、各認証サーバに特別の機能が備わっていなくても、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能な認証システムおよび認証方法の提供を目的とする。

【０００６】

【課題を解決するための手段】上述の目的を達成するため、請求項１にかかる発明は、通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとを具備する認証システムであって、上記認証サーバは、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、上記プロキシサーバは、接続先から上記クライアントに証明書を要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、上記クライアントは、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信する構成としてある。

【０００７】すなわち、クライアント、複数のプロキシサーバ、複数の認証サーバは、通信回線を介して双方向通信可能に接続されている。複数のプロキシサーバは、クライアントとサーバとの間に介在して、クライアントとサーバとを接続させることが可能である。複数の認証サーバは、それぞれのプロキシサーバに対応して設けられており、対応するプロキシサーバとこのプロキシサーバの接続元との間の認証を行う。なお、クライアントに最も近いプロキシサーバの接続元はクライアントであり、それ以外のプロキシサーバの接続元は別のプロキシサーバとなる。

【０００８】認証サーバは、予め、対応するプロキシサーバとこの接続元に証明書を配布する。その上で、配布した証明書に基づいて、複数の認証サーバが対応するプロキシサーバとこの接続元との間の認証をクライアント側から順番に行う。その際、この認証サーバから対応するプロキシサーバとこの接続元とに配布された証明書を確認することで、プロキシサーバとこの接続元との間の認証を行う。

【０００９】クライアントとサーバとを中継するプロキシサーバは、接続先からクライアントに証明書を要求する証明書要求が入力されたとき、この証明書要求を接続元へ送信する。接続元が別のプロキシサーバであれば、接続先のプロキシサーバと同様、入力された証明書要求を接続元へ送信する。そして、接続元がクライアントとなったとき、クライアントはこの証明書要求に応じて、自らに配布されるとともに、認証済みの証明書を接続先のプロキシサーバへ送信する。すると、クライアントに最も近いプロキシサーバは、この認証済みの証明書を入手して接続先へ送信する。接続先がプロキシサーバであれば、接続元のプロキシサーバと同様、この認証済みの証明書を入手して接続先へ送信する。

【００１０】すなわち、クライアントに配布された証明書は、認証されるとともに、クライアントとサーバとを中継する複数のプロキシサーバに受け渡されることになる。すると、各プロキシサーバにて、クライアントが保有する認証済みの証明書を確認することが可能となる。したがって、すべての認証サーバにクライアントを使用するユーザを登録する必要がなく、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能となる。その際、登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能は不要である。

【００１１】ここで、クライアントに証明書を要求する証明書要求の出力元は様々可能であり、その具体的な構成の一例として、請求項２にかかる発明は、請求項１に記載の認証システムにおいて、上記サーバに最も近いプロキシサーバは、接続元との間の認証が完了したとき、この接続元へ上記証明書要求を送信する構成としてある。すなわち、サーバに最も近いプロキシサーバとこの接続元のプロキシサーバとの間の認証が完了したとき、サーバに最も近いプロキシサーバが証明書要求を接続元へ送信する。すると、サーバに最も近いプロキシサーバとクライアントとを中継するプロキシサーバが、この証明書要求をクライアントまで送信する。したがって、サーバに最も近いプロキシサーバにて、クライアントを使用するユーザの認証を行うことが可能となる。むろん、証明書要求の出力元がサーバに最も近いプロキシサーバである構成は一例に過ぎず、他のプロキシサーバが出力元であってもよいし、外部のサーバが出力元であってもよく、様々可能である。

【００１２】認証サーバが配布する証明書は、クライアントやプロキシサーバを識別する情報であればよい。また、プロキシサーバに受け渡す証明書はクライアントに配布された証明書に限定されず、その構成の一例として、請求項３にかかる発明は、請求項１あるいは請求項２のいずれかに記載の認証システムにおいて、上記プロキシサーバは、上記クライアントに配布された上記証明書とあわせて、自らに配布された上記証明書を接続先へ送信する構成としてある。すなわち、プロキシサーバは、クライアントが保有する認証済みの証明書とあわせて他のプロキシサーバが保有する認証済みの証明書を確認することができる。したがって、より確実に認証を行うことができる。

【００１３】また、各プロキシサーバに配布された証明

書をさらに活用する構成の一例として、請求項４にかかる発明は、請求項１～請求項３のいずれかに記載の認証システムにおいて、上記プロキシサーバは、自らに配布された上記証明書を上記証明書要求に添付して接続元へ送信し、上記クライアントは、上記プロキシサーバに配布された上記証明書を確認して、配布された上記証明書を接続先へ送信する構成としてある。すなわち、クライアントは、プロキシサーバが保有する認証済みの証明書を受け取る。そして、受け取った証明書を確認したうえで、自らが保有する証明書をプロキシサーバに引き渡す。したがって、より確実に認証を行うことができる。

【００１４】ところで、認証システムを構成するクライアント、複数のプロキシサーバ、認証サーバは通信回線により接続されているため、通信回線等の状態によっては認証するのに時間がかかりすぎることがある。そこで、請求項５にかかる発明は、請求項１～請求項４のいずれかに記載の認証システムにおいて、上記クライアントは、上記サーバへの接続を要求してから所定時間内に上記証明書要求を入手することができないとき、自らに配布された証明書の引き渡しを中止する構成としてある。すなわち、クライアントは、接続先のプロキシサーバから証明書要求が所定時間内に送信されない場合、自らが保有する証明書の引き渡しを中止する。したがって、通信の状態が良好でない等の場合にサーバへの接続処理が中止されるため、本システムの利用価値をより高めることができる。

【００１５】上述したように、クライアント、プロキシサーバ、認証サーバとからなるシステムにおいては、所定のプログラムが実行され、このプログラムは上述の手段に対応した所定の制御手順に従って処理を進めていく上で、その根底にはその手順に発明が存在するということは当然である。

【００１６】そこで、請求項６にかかる発明は、通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとにより構成される認証方法であって、上記認証サーバにて、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、上記プロキシサーバにて、接続先から上記クライアントに証明書を要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、上記クライアントにて、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信することで認証を行う構成としてある。すなわち、必ずしも実体のあるシステムに限らず、その方法としても有効であり、基本的には同様の作用となる。また、請求項２～請求項５に記載されたシステム構成を当該方法に対応させることも可能であることは言うまでもない。

【００１７】

【発明の実施の形態】以下、図面にもとづいて本発明の実施形態を説明する。図１は、本発明の一実施形態にかかる認証システムを概略図により示している。図１において、認証システム１００は、双方向通信可能な通信回線に接続されたクライアント１０、プロキシサーバ２１，２２、認証サーバ３１，３２とから構成されている。ユーザが、クライアント１０からＡＰサーバ４０へ接続を要求すると、所定の認証が完了した後、プロキシサーバ２１，２２を介してクライアント１０とＡＰサーバ４０との接続が確立するようになっている。

【００１８】クライアント１０は、通信回線にアクセス可能な通信インタフェースを備え、通信回線に接続可能なコンピュータであればよい。そこで、クライアント１０は、例えば各家庭で汎用的に用いられるパーソナルコンピュータであってもよいし、持ち運びの可能な携帯端末であってもよい。また、通信回線には所定のパーソナルコンピュータをローカルサーバにするなどしてＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を接続することも可能である。すなわち、クライアント１０の代わりにＬＡＮを接続し、このＬＡＮ内の複数のパーソナルコンピュータから通信回線にアクセスする構成としてもよい。

【００１９】本実施形態のクライアント１０は、所定のＯＳプログラムやアプリケーションプログラムを記憶するハードディスクを備えている。そして、ＣＰＵ、ＲＯＭ、ＲＡＭ等によってこれらのＯＳプログラムやアプリケーションプログラムを実行する。また、ディスプレイ、キーボード、マウス等も備えており、ＯＳプログラムの制御によりこれらを駆動している。

【００２０】プロキシサーバ２１，２２は、クライアント１０とＡＰサーバ４０との間に介在して、クライアントとサーバとを接続させることが可能である。そのため、プロキシサーバ２１，２２は、通信回線にアクセス可能な通信インタフェースや、所定のプログラムを記憶するハードディスク等を備えたハードウェア構成となっている。そして、ＣＰＵ、ＲＯＭ、ＲＡＭ等によってハードディスクに記憶されているプログラムを実行する。

【００２１】認証サーバ３１，３２は、それぞれのプロキシサーバ２１，２２に対応して設けられており、対応するプロキシサーバ２１，２２とこのプロキシサーバ２１，２２の接続元との間の認証を行う。ここで、プロキシサーバ２１の接続元はクライアント１０であり、認証サーバ３１がクライアント１０とプロキシサーバ２１との間の認証を行う。また、プロキシサーバ２２の接続元はプロキシサーバ２１であり、認証サーバ３２がプロキシサーバ２１とプロキシサーバ２２との間の認証を行

う。なお、認証サーバ３１，３２のハードウェアの構成は、プロキシサーバ２１，２２と概略同様となっている。

【００２２】認証サーバ３１，３２は、予め、対応するプロキシサーバ２１，２２とこの接続元になるクライアント１０あるいはプロキシサーバ２１とのユーザ登録を受け付ける。そして、クライアント１０あるいはプロキシサーバ２１，２２に証明書を配布する。

【００２３】本実施形態の場合、クライアント１０からＡＰサーバ４０へと接続を要求するユーザのユーザ情報は、クライアント１０に最も近いプロキシサーバ２１の属する認証サーバ３１に登録される。認証サーバ３１からは、ユーザの証明書３１ａがクライアント１０に配布される。また、プロキシサーバ２１としてのユーザ情報は、プロキシサーバ２１の属する認証サーバ３１と、次に中継されるプロキシサーバ２２の属する認証サーバ３２に登録される。認証サーバ３１からは証明書３１ｂが配布され、認証サーバ３２から証明書３２ａが配布される。プロキシサーバ２２としてのユーザ情報は認証サーバ３２に登録され、認証サーバ３２から証明書３２ｂが配布される。

【００２４】その上で、配布した証明書３１ａ，３１ｂ，３２ａ，３２ｂに基づいて、認証サーバ３１，３２が対応するプロキシサーバ２１，２２とこの接続元との間の認証をクライアント側から順番に行う。ユーザがクライアント１０からＡＰサーバ４０へ接続要求を行うと、まず、認証サーバ３１が証明書３１ａと証明書３１ｂとを入手して認証を行う。この認証が成功すれば、プロキシサーバ２１からプロキシサーバ２２へ接続され、認証サーバ３２が証明書３２ａと証明書３２ｂとを入手して認証を行う。この認証が成功すると、所定の手順により、ＡＰサーバ４０に最も近いプロキシサーバ２２が保有する証明書３２ｂと、クライアント１０が保有する証明書３１ａとを、プロキシサーバ２１を介して交換する。

【００２５】ここで、クライアント１０とプロキシサーバ２１との間は、証明書３１ａと証明書３１ｂとにより認証された状態である。また、プロキシサーバ２１とプロキシサーバ２２との間も、証明書３２ａと証明書３２ｂとにより認証された状態である。すなわち、クライアント１０とプロキシサーバ２２との間は、プロキシサーバ２１を介して認証済みの状態となっている。すると、交換された証明書３２ｂ、証明書３１ａは互いに信頼できる証明書である。そこで、プロキシサーバ２２は、クライアント１０を使用するユーザの証明書３１ａに基づいてＡＰサーバ４０に接続を要求すると、クライアント１０とＡＰサーバ４０との接続も確立させることが可能となる。

【００２６】したがって、ユーザ登録をクライアント１０に最も近いプロキシサーバ２１に対応する認証サーバ３１でのみ行うことで、各プロキシサーバにてユーザの認証を行うことが可能となる。その際、認証サーバ間でユーザの証明書を受け渡す必要がない。なお、クライアント１０とプロキシサーバ２２との間が認証済みの状態となったときに、クライアント１０が保有する証明書３１ａだけをプロキシサーバ２１を介してプロキシサーバ２２に受け渡すだけでもよい。この場合でも、証明書３１ａは信頼できる証明書であるため、この証明書３１ａを用いて各プロキシサーバにてユーザの認証を行うことが可能である。

【００２７】次に、本認証システム１００におけるクライアント１０、プロキシサーバ２１，２２にて実行される処理をフローチャートに沿って説明する。なお、本フローでは、プロキシサーバ２１が保有する証明書３１ｂ，３２ａもクライアント１０あるいはプロキシサーバ２２に受け渡すことでより確実に認証を行う構成としている。図２、図３、図４は、それぞれクライアント１０、プロキシサーバ２１、プロキシサーバ２２にて実行される処理の概略を示すフローチャートである。

【００２８】まず、ユーザがクライアント１０からＡＰサーバ４０へ接続要求を行うと（図２のステップＳ１００）、プロキシサーバ２１はクライアント１０からＡＰサーバ４０への接続要求を受信する（図３のステップＳ２００）。そして、プロキシサーバ２１は、接続してきたユーザの認証を認証サーバ３１へ要求する（ステップＳ２０５）。認証サーバ３１から認証結果を受信すると（ステップＳ２１０）、ユーザの認証が成功かどうかを判断する（ステップＳ２１５）。認証が失敗であれば、ユーザからＡＰサーバ４０への接続要求を拒否するとともに、接続要求拒否をクライアント１０に通知し（ステップＳ２２０）、本フローを終了する。この場合、クライアント１０では図示しないフローにて図２のフローを終了する。認証が成功であれば、接続先のプロキシサーバ２２へＡＰサーバ４０への接続要求を行う（ステップＳ２２５）。

【００２９】プロキシサーバ２２は、プロキシサーバ２１からＡＰサーバ４０への接続要求を受信すると（図４のステップＳ３００）、接続してきたプロキシサーバ２１の認証を認証サーバ３２へ要求する（ステップＳ３０５）。認証サーバ３２からその認証結果を受信すると（ステップＳ３１０）、プロキシサーバ２１の認証が成功かどうかを判断する（ステップＳ３１５）。認証が失敗であれば、プロキシサーバ２１からＡＰサーバ４０への接続要求を拒否するとともに、接続要求拒否をプロキシサーバ２１に通知し（ステップＳ３２０）、図４のフローを終了する。この場合、プロキシサーバ２１では図示しないフローで接続要求拒否をクライアント１０に通知し、図３のフローを終了する。認証が成功であれば、プロキシサーバ２２は、接続元のプロキシサーバ２１に対して、ＡＰサーバ４０へ接続要求を行っているユーザ

の証明書要求を送信する（ステップＳ３２５）。その際、自らが保有する認証済みの証明書３２ｂを添付している。

【００３０】すると、プロキシサーバ２１は、プロキシサーバ２２から、ＡＰサーバ４０へ接続要求を行っているユーザの証明書要求を受信する（図３のステップＳ２３０）。そして、認証サーバ３２で認証済みの証明書３２ｂが添付されていることを確認する（ステップＳ２３５）。その上で、プロキシサーバ２１はクライアント１０に対して、ＡＰサーバ４０へ接続要求を行っているユーザの証明書要求を送信する（ステップＳ２４０）。その際、証明書３２ｂとあわせて、プロキシサーバ２１が保有する認証済みの証明書３１ｂをさらに添付している。

【００３１】クライアント１０では、プロキシサーバ２１から、所定時間内にＡＰサーバ４０へ接続要求を行っているユーザの証明書要求を受信したかどうかを判断する（図２のステップＳ１０５）。プロキシサーバ２１から接続要求拒否が通知されるか、所定時間内にユーザの証明書要求を受信しなかった場合は、ＡＰサーバ４０への接続要求を取り消す。したがって、通信の状態が良好でない等の場合に、ＡＰサーバ４０への接続要求を必要以上に長時間行うことがない。

【００３２】ユーザの証明書要求を受信した場合（ステップＳ１１０）、プロキシサーバ２１に配布された証明書３１ｂが添付されているとともに、認証サーバ３１で認証済みであることを確認する（ステップＳ１１５）。また、証明書要求元であるＡＰサーバ４０に最も近いプロキシサーバ２２に配布された証明書３２ｂが添付されているとともに、認証サーバ３２で認証済みであることを確認する（ステップＳ１２０）。そこで、クライアント１０は、プロキシサーバ２１に対して、ＡＰサーバ４０へ接続要求を行っているユーザの証明書３１ａを送信し（ステップＳ１２５）、図２のフローを終了する。

【００３３】プロキシサーバ２１では、クライアント１０から、ＡＰサーバ４０へ接続要求を行っているユーザの証明書３１ａを受信する（図３のステップＳ２４５）。そして、証明書３１ａが認証サーバ３１で認証済みであることを確認する（ステップＳ２５０）。その上で、プロキシサーバ２２に対して、ＡＰサーバ４０へ接続要求を行っているユーザの証明書３１ａを送信し（ステップＳ２５５）、図３のフローを終了する。その際、プロキシサーバ２１に配布された認証済みの証明書３２ａをさらに添付している。

【００３４】プロキシサーバ２２では、プロキシサーバ２１から、ＡＰサーバ４０へ接続要求を行っているユーザの証明書３１ａを受信する（図４のステップＳ３３０）。そして、認証サーバ３２で認証済みの証明書３２ａが添付されていることを確認する（ステップＳ３３５）。また、ＡＰサーバ４０へ接続要求を行っているユーザの証明書３１ａも認証済みであることを確認する（ステップＳ３４０）。その結果、プロキシサーバ２２とユーザとが相互に認証できたこととなり、プロキシサーバ２２はＡＰサーバ４０へ接続要求を送信する（ステップＳ３４５）。すると、プロキシサーバ２１，２２を介してクライアント１０とＡＰサーバ４０との接続を確立させることが可能である。

【００３５】このように、本認証システム１００では、配布された証明書に基づいて、認証サーバにて対応するプロキシサーバとこの接続元との間の認証がクライアント側から順番に行われる。そして、クライアント１０に配布された証明書３１ａがプロキシサーバ２１を介してＡＰサーバ４０に最も近いプロキシサーバ２２に受け渡される。したがって、すべての認証サーバにクライアントを使用するユーザを登録する必要がなく、各プロキシサーバにてユーザを認証することが可能となる。その際、登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能は不要である。

【００３６】また、クライアントは、各プロキシサーバが保有する認証済みの証明書を受け取って確認したうえで、自らが保有する認証済みの証明書をプロキシサーバに引き渡す。さらに、クライアントとサーバに最も近いプロキシサーバとを中継するプロキシサーバが保有する認証済みの証明書も、クライアントやサーバに最も近いプロキシサーバに受け渡され、確認される。したがって、より確実に認証が行われる。

【００３７】なお、本発明は、クライアントとサーバとを中継するプロキシサーバが三台以上ある場合にも適用することが可能である。図５は、変形例にかかる認証システムを概略図により示している。図５において、認証システム２００は、クライアント１０、プロキシサーバ２１，２３，２２、認証サーバ３１，３３，３２とから構成されている。すなわち、クライアント１０とＡＰサーバ４０とを中継するプロキシサーバは三台あり、このプロキシサーバに対応して設けられている認証サーバも三台あることになる。なお、新たに設けられているプロキシサーバ２３、認証サーバ３３のハードウェア構成は概略他のプロキシサーバ、認証サーバと同様であるので、説明を省略する。

【００３８】認証システム２００では、認証サーバ３１が、クライアント１０に証明書３１ａを配布し、プロキシサーバ２１に証明書３１ｂを配布している。また、認証サーバ３３は、プロキシサーバ２１に証明書３３ａを配布し、プロキシサーバ２３に証明書３３ｂを配布している。そして、認証サーバ３２が、プロキシサーバ２３に証明書３２ａを配布し、プロキシサーバ２２に証明書３２ｂを配布している。

【００３９】以下、本認証システム２００におけるクライアント１０、プロキシサーバ２１，２３，２２にて実行される処理をフローチャートに沿って説明する。図

６、図７、図８は、それぞれプロキシサーバ２１、プロキシサーバ２３、プロキシサーバ２２にて実行される処理の概略を示すフローチャートである。なお、クライアント１０で実行される処理の概略は図２と同様である。

【００４０】まず、ユーザがクライアント１０からＡＰサーバ４０へ接続要求を行うと（図２のステップＳ１００）、プロキシサーバ２１はクライアント１０からＡＰサーバ４０への接続要求を受信する（図６のステップＳ４００）。そして、プロキシサーバ２１は、ユーザの認証を認証サーバ３１へ要求する（ステップＳ４０５）。認証サーバ３１から認証結果を受信すると（ステップＳ４１０）、ユーザの認証が成功かどうかを判断する（ステップＳ４１５）。認証が失敗であれば、ユーザからの接続要求を拒否するとともに、接続要求拒否をクライアント１０に通知し（ステップＳ４２０）、本フローを終了する。この場合、クライアント１０では図示しないフローにて図２のフローを終了する。認証が成功であれば、プロキシサーバ２１はプロキシサーバ２３へＡＰサーバ４０への接続要求を行う（ステップＳ４２５）。

【００４１】プロキシサーバ２３は、プロキシサーバ２１からＡＰサーバ４０への接続要求を受信すると（図７のステップＳ５００）、プロキシサーバ２１の認証を認証サーバ３３へ要求する（ステップＳ５０５）。認証サーバ３３からその認証結果を受信すると（ステップＳ５１０）、プロキシサーバ２１の認証が成功かどうかを判断する（ステップＳ５１５）。認証が失敗であれば、ＡＰサーバ４０への接続要求を拒否するとともに、接続要求拒否をプロキシサーバ２１に通知し（ステップＳ５２０）、図７のフローを終了する。この場合、プロキシサーバ２１では図示しないフローで接続要求拒否をクライアント１０に通知し、図６のフローを終了する。認証が成功であれば、接続先にさらにプロキシサーバ２２があるため、プロキシサーバ２２へＡＰサーバ４０への接続要求を行う（ステップＳ５２５）。

【００４２】プロキシサーバ２２は、プロキシサーバ２３からＡＰサーバ４０への接続要求を受信すると（図８のステップＳ６００）、プロキシサーバ２３の認証を認証サーバ３２へ要求する（ステップＳ６０５）。認証サーバ３２からその認証結果を受信すると（ステップＳ６１０）、プロキシサーバ２３の認証が成功かどうかを判断する（ステップＳ６１５）。認証が失敗であれば、ＡＰサーバ４０への接続要求を拒否するとともに、接続要求拒否をプロキシサーバ２３に通知し（ステップＳ６２０）、図８のフローを終了する。この場合、接続要求拒否の通知は、さらにプロキシサーバ２１、クライアント１０の順に伝達され、図７と図６のフローは終了する。認証が成功であれば、自らが保有する認証済みの証明書３２ｂを添付して、接続元のプロキシサーバ２３にユーザの証明書要求を送信する（ステップＳ６２５）。

【００４３】すると、プロキシサーバ２３は、プロキシサーバ２２から、ユーザの証明書要求を受信する（図７のステップＳ５３０）。そして、認証サーバ３２で認証済みの証明書３２ｂが添付されていることを確認する（ステップＳ５３５）。その上で、さらに認証済みの証明書３３ｂを添付して、プロキシサーバ２３は接続元のプロキシサーバ２１にユーザの証明書要求を送信する（ステップＳ５４０）。プロキシサーバ２１では、プロキシサーバ２３から、ユーザの証明書要求を受信する（図５のステップＳ４３０）。そして、認証サーバ３３で認証済みの証明書３３ｂが添付されていることを確認する（ステップＳ４３５）。その上で、さらに認証済みの証明書３１ｂを添付して、プロキシサーバ２３は接続元のプロキシサーバ２１にユーザの証明書要求を送信する（ステップＳ４４０）。

【００４４】クライアント１０では、プロキシサーバ２１から、所定時間内にユーザの証明書要求を受信したかどうかを判断する（図２のステップＳ１０５）。プロキシサーバ２１から接続要求拒否が通知されるか、所定時間内にユーザの証明書要求を受信しなかった場合は、ＡＰサーバ４０への接続要求を取り消す。ユーザの証明書要求を受信した場合（ステップＳ１１０）、プロキシサーバ２１が保有する認証済みの証明書３１ｂを確認する（ステップＳ１１５）。また、プロキシサーバ２３が保有する認証済みの証明書３３ｂを確認する。さらに、証明書要求元であるＡＰサーバ４０に最も近いプロキシサーバ２２に配布された証明書３２ｂが添付されているとともに、認証サーバ３２で認証済みであることを確認する（ステップＳ１２０）。その上で、クライアント１０は、プロキシサーバ２１にユーザの証明書３１ａを送信し（ステップＳ１２５）、図２のフローを終了する。

【００４５】プロキシサーバ２１では、クライアント１０からユーザの証明書３１ａを受信し（図６のステップＳ４４５）、証明書３１ａが認証サーバ３１で認証済みであることを確認する（ステップＳ４５０）。そして、プロキシサーバ２１に配布された認証済みの証明書３２ａをさらに添付して、プロキシサーバ２２にユーザの証明書３１ａを送信し（ステップＳ４５５）、図６のフローを終了する。プロキシサーバ２３では、接続元のプロキシサーバ２１からユーザの証明書３１ａを受信し（図７のステップＳ５４５）、認証サーバ３３で認証済みの証明書３３ａが添付されていることを確認する（ステップＳ５５０）。そして、プロキシサーバ２３に配布された認証済みの証明書３３ａをさらに添付して、プロキシサーバ２２にユーザの証明書３１ａを送信し（ステップＳ５５５）、図７のフローを終了する。

【００４６】プロキシサーバ２２では、プロキシサーバ２３からユーザの証明書３１ａを受信し（図８のステップＳ６３０）、プロキシサーバ２３が保有する認証済みの証明書３２ａが添付されていることを確認する（ステップＳ６３５）。また、プロキシサーバ２１が保有する

証明書３３ａを確認する。そして、ユーザの証明書３１ａも確認する（ステップＳ６４０）。その結果、プロキシサーバ２２とユーザとが相互に認証できたこととなり、プロキシサーバ２２はＡＰサーバ４０へ接続要求を送信する（ステップＳ６４５）。すると、プロキシサーバ２１，２３，２２を介してクライアント１０とＡＰサーバ４０との接続を確立させることが可能である。

【００４７】このように、クライアントとサーバを中継するプロキシサーバが三台ある本認証システム２００でも、すべての認証サーバにユーザを登録する必要がなく、各プロキシサーバにてクライアントを認証することが可能である。また、登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能も不要である。また、中継するプロキシサーバが四台以上ある認証システムであっても、プロキシサーバ間に介在するプロキシサーバ２３と同様の処理を行うことにより、上述の認証を行うことが可能となる。

【００４８】

【発明の効果】以上説明したように、本発明は、登録されたユーザの証明書を認証サーバ間で受け渡す必要なく、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能な認証システムを提供することができる。また、請求項２にかかる発明によれば、サーバに最も近いプロキシサーバにて、クライアントを使用するユーザの認証を行うことが可能となる。さらに、請求項３にかかる発明によれば、プロキシサーバは、他のプロキシサーバが保有する認証済みの証明書も確認することができるので、より確実に認証を行うことが可能となる。

【００４９】さらに、請求項４にかかる発明によれば、クライアントはプロキシサーバが保有する認証済みの証明書を確認することができるので、より確実に認証を行うことが可能となる。さらに、請求項５にかかる発明によれば、本システムの利用価値をより高めることができる。さらに、請求項６にかかる発明によれば、登録されたユーザの証明書を認証サーバ間で受け渡す必要なく、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能な認証方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態にかかる認証システムを示す概略図である。

【図２】クライアントにて実行される処理の概略を示すフローチャートである。

【図３】クライアントとプロキシサーバを中継するプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図４】サーバに最も近いプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図５】変形例にかかる認証システムを示す概略図である。

【図６】クライアントとプロキシサーバを中継するプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図７】プロキシサーバどうしを中継するプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図８】サーバに最も近いプロキシサーバにて実行される処理の概略を示すフローチャートである。

【符号の説明】

１０　クライアント

１００，２００　認証システム

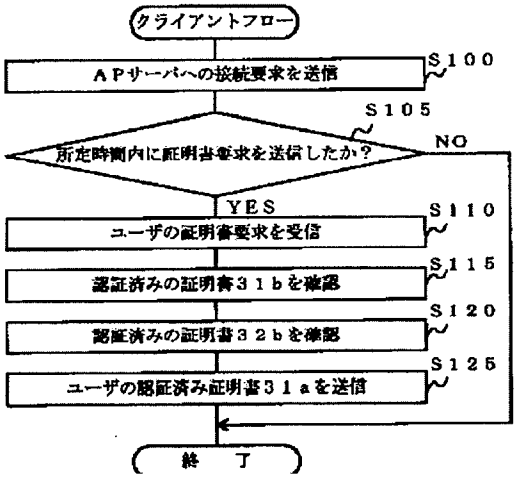
２１，２２，２３　プロキシサーバ

３１，３２，３３　認証サーバ

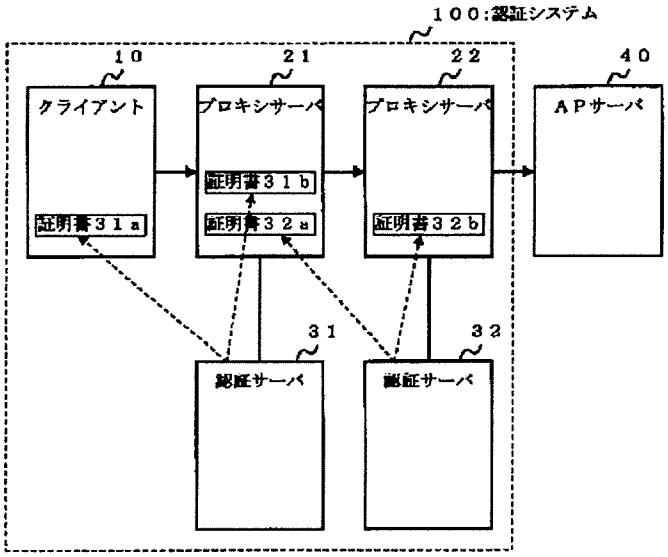
３１ａ，３１ｂ，３２ａ，３２ｂ，３３ａ，３３ｂ　証明書

４０　ＡＰサーバ

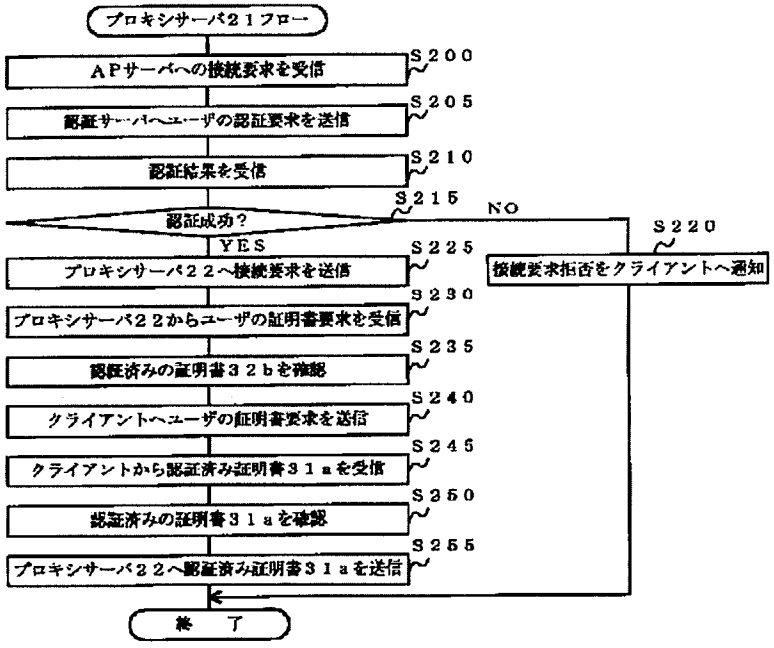
【図２】



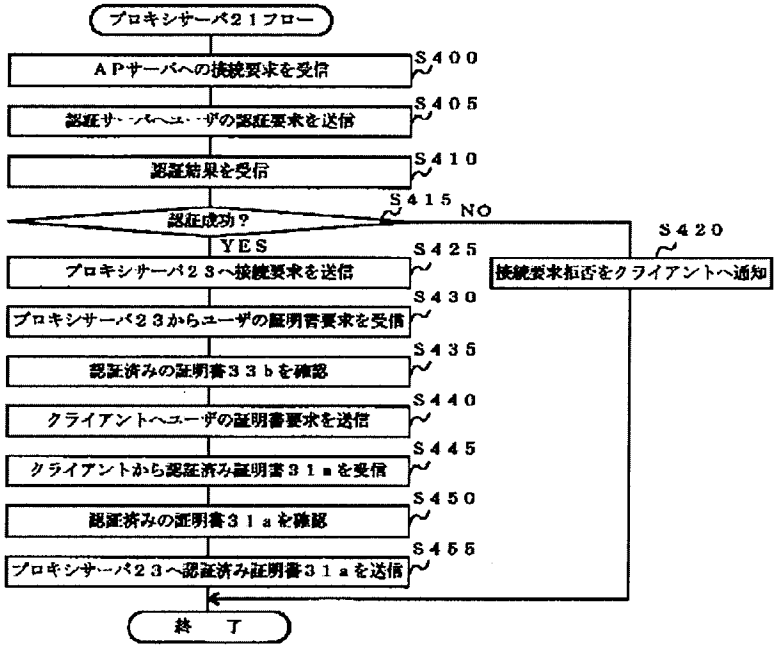
【図１】


１００:認証システム
１０
２１
２２
４０
クライアント
プロキシサーバ
プロキシサーバ
ＡＰサーバ
証明書３１ｂ
証明書３１ａ
証明書３２ａ
証明書３２ｂ
３１
３２
認証サーバ
認証サーバ

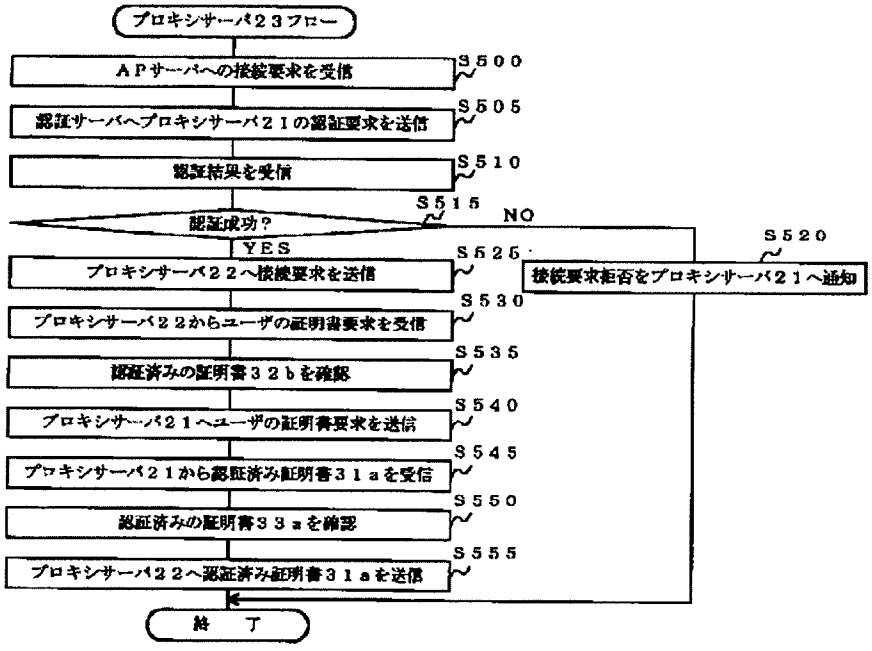
【図３】


プロキシサーバ２１フロー
ＡＰサーバへの接続要求を受信
Ｓ２００
認証サーバへユーザの認証要求を送信
Ｓ２０５
認証結果を受信
Ｓ２１０
認証成功?
Ｓ２１５
NO
Ｓ２２０
接続要求拒否をクライアントへ通知
YES
プロキシサーバ２２へ接続要求を送信
Ｓ２２５
プロキシサーバ２２からユーザの証明書要求を受信
Ｓ２３０
認証済みの証明書３２ｂを確認
Ｓ２３５
クライアントへユーザの証明書要求を送信
Ｓ２４０
クライアントから認証済み証明書３１ａを受信
Ｓ２４５
認証済みの証明書３１ａを確認
Ｓ２５０
プロキシサーバ２２へ認証済み証明書３１ａを送信
Ｓ２５５
終　了

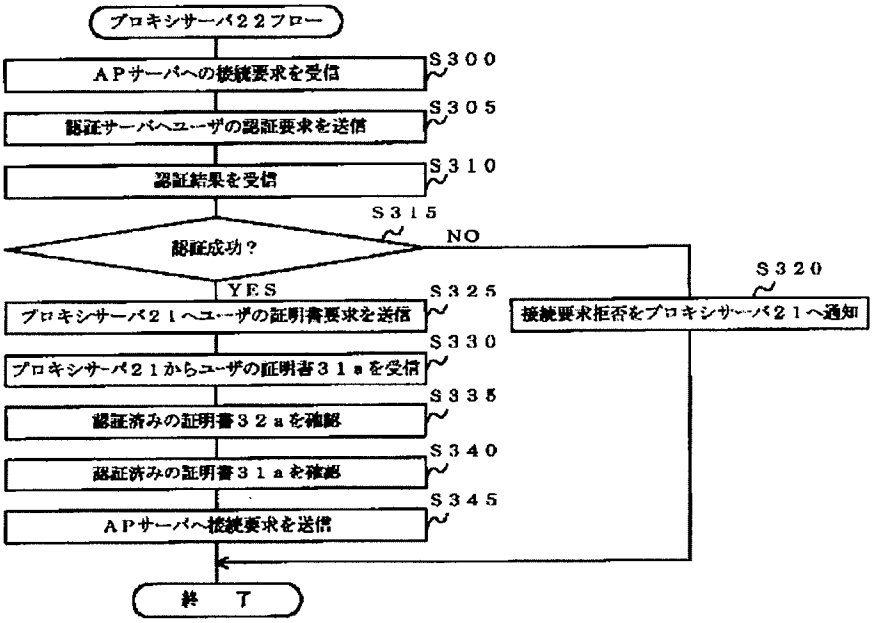
【図６】


プロキシサーバ２１フロー
ＡＰサーバへの接続要求を受信
Ｓ４００
認証サーバへユーザの認証要求を送信
Ｓ４０５
認証結果を受信
Ｓ４１０
認証成功？
Ｓ４１５
NO
YES
Ｓ４２０
接続要求拒否をクライアントへ通知
Ｓ４２５
プロキシサーバ２３へ接続要求を送信
Ｓ４３０
プロキシサーバ２３からユーザの証明書要求を受信
Ｓ４３５
認証済みの証明書３３ｂを確認
Ｓ４４０
クライアントへユーザの証明書要求を送信
Ｓ４４５
クライアントから認証済み証明書３１ａを受信
Ｓ４５０
認証済みの証明書３１ａを確認
Ｓ４５５
プロキシサーバ２３へ認証済み証明書３１ａを送信
終　了

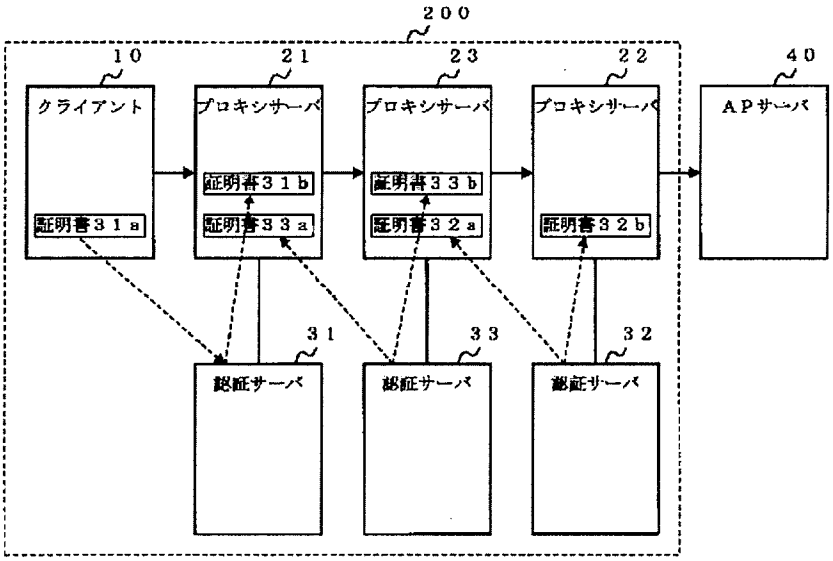
【図７】


プロキシサーバ２３フロー
ＡＰサーバへの接続要求を受信
Ｓ５００
認証サーバへプロキシサーバ２１の認証要求を送信
Ｓ５０５
認証結果を受信
Ｓ５１０
認証成功？
Ｓ５１５
NO
YES
Ｓ５２０
接続要求拒否をプロキシサーバ２１へ通知
Ｓ５２５
プロキシサーバ２２へ接続要求を送信
Ｓ５３０
プロキシサーバ２２からユーザの証明書要求を受信
Ｓ５３５
認証済みの証明書３２ｂを確認
Ｓ５４０
プロキシサーバ２１へユーザの証明書要求を送信
Ｓ５４５
プロキシサーバ２１から認証済み証明書３１ａを受信
Ｓ５５０
認証済みの証明書３３ａを確認
Ｓ５５５
プロキシサーバ２２へ認証済み証明書３１ａを送信
終　了

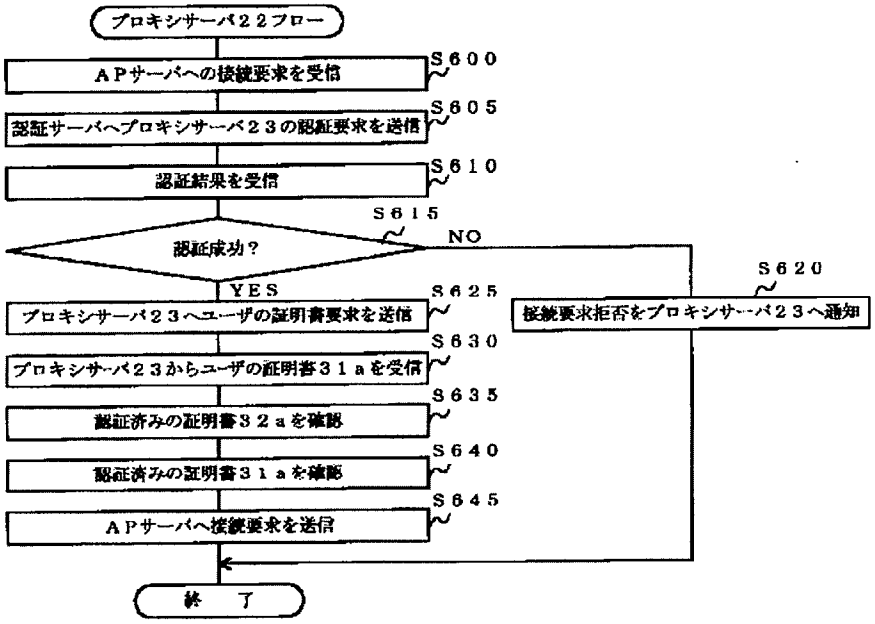
【図４】


プロキシサーバ２２フロー
ＡＰサーバへの接続要求を受信
Ｓ３００
認証サーバへユーザの認証要求を送信
Ｓ３０５
認証結果を受信
Ｓ３１０
Ｓ３１５
認証成功？
ＮＯ
ＹＥＳ
Ｓ３２０
接続要求拒否をプロキシサーバ２１へ通知
Ｓ３２５
プロキシサーバ２１へユーザの証明書要求を送信
Ｓ３３０
プロキシサーバ２１からユーザの証明書３１ａを受信
Ｓ３３５
認証済みの証明書３２ａを確認
Ｓ３４０
認証済みの証明書３１ａを確認
Ｓ３４５
ＡＰサーバへ接続要求を送信
終　了

【図５】


２００
１０
２１
２３
２２
４０
クライアント
プロキシサーバ
プロキシサーバ
プロキシサーバ
ＡＰサーバ
証明書３１ｂ
証明書３３ｂ
証明書３１ａ
証明書３３ａ
証明書３２ａ
証明書３２ｂ
３１
３３
３２
認証サーバ
認証サーバ
認証サーバ

【図８】


プロキシサーバ２２フロー
ＡＰサーバへの接続要求を受信
Ｓ６００
認証サーバへプロキシサーバ２３の認証要求を送信
Ｓ６０５
認証結果を受信
Ｓ６１０
Ｓ６１５
認証成功？
NO
YES
Ｓ６２０
接続要求拒否をプロキシサーバ２３へ通知
Ｓ６２５
プロキシサーバ２３へユーザの証明書要求を送信
Ｓ６３０
プロキシサーバ２３からユーザの証明書３１ａを受信
Ｓ６３５
認証済みの証明書３２ａを確認
Ｓ６４０
認証済みの証明書３１ａを確認
Ｓ６４５
ＡＰサーバへ接続要求を送信
終　了